

**ANALISA MODIFIKASI ALGORITMA RC4 MENGGUNAKAN *TWO STATE TABLES* DAN *INITIAL STATE FACTORIAL* UNTUK PENGAMANAN FILE**

**SKRIPSI**

Diajukan Untuk Memenuhi  
Persyaratan Guna Meraih Gelar Sarjana Strata 1  
Teknik Informatika Universitas Muhammadiyah Malang



**Barkie Hasni Azzaky**  
**201310370311299**

**JURUSAN TEKNIK INFORMATIKA**  
**FAKULTAS TEKNIK**  
**UNIVERSITAS MUHAMMADIYAH MALANG**  
**2018**

## LEMBAR PERSETUJUAN

### **ANALISA MODIFIKASI ALGORITMA RC4 MENGGUNAKAN *TWO* *STATE TABLES* DAN *INITIAL STATE FACTORIAL* UNTUK PENGAMANAN FILE**

#### SKRIPSI

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1  
Teknik Informatika Universitas Muhammadiyah Malang

Disusun oleh:

**BARKIE HASNI AZZAKY**

**201310370311299**

Menyetujui,

Pembimbing I



**Aminudin, S.Kom., M.Cs**  
**NIDN. 0701068603**

Pembimbing II



**Sofyan Arifianto, S.Si., M.T**  
**NIDN. 0721038309**

## **LEMBAR PENGESAHAN**

### **ANALISA MODIFIKASI ALGORITMA RC4 MENGGUNAKAN *TWO* *STATE TABLES* DAN *INITIAL STATE FACTORIAL* UNTUK PENGAMANAN FILE**

#### **TUGAS AKHIR**

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1  
Teknik Informatika Universitas Muhammadiyah Malang

Disusun Oleh:

**BARKIE HASNI AZZAKY**

**201310370311299**

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji  
pada tanggal 25 Juli 2018

Menyetujui,


Penguji I

Penguji II



**Denar Regata Akbi, S.KOm, M.Kom**

**NIDN. 0701058601**

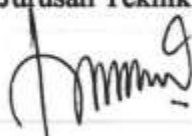


**Fauzi Dwi Setiawan S, S.T, M.ComSc**

**NIDN. 18930706199**

Mengetahui,

Ketua Jurusan Teknik Informatika



**Gita Indah Marthasari, S.T, M.Kom**

**NIDN. 0720038101**

## LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Barkie Hasni Azzaky  
Tempat, Tanggal Lahir : Lamongan, 13 Desember 1993  
NIM : 201310370311299  
Fakultas / Jurusan : Teknik / Teknik Informatika

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul "**Analisa Modifikasi Algoritma RC4 Menggunakan *Two State Tables* dan *Initial State Factorial* untuk Pengamanan File**" beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun keseluruhan, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko / sanksi yang berlaku.

Malang, 13 Juli 2018

Yang Membuat Pernyataan

**BARKIE HASNI AZZAKY**

Mengetahui,

Pembimbing I



**Aminudin, S.Kom., M.Cs**  
NIDN. 0701068603

Pembimbing II



**Sofyan Arifianto, S.Si., M.T**  
NIDN. 0721038309

## LEMBAR PERSEMBAHAN

Sembah sujud serta syukur panjatkan kepada kehadiran Allah SWT, Dzat yang Maha Berilmu diatas mereka yang merasa diri berilmu, serta pencipta Maha Sempurna diatas segala yang dianggap sempurna. Taburan cinta dan kasih sayang-Mu telah memberikan kekuatan, membekaliku dengan ilmu serta memperkenalkanku dengan cinta. Atasa karunia serta kemudahan yang Engkau berikan akhirnya skripsi yang sederhana ini dapat terselesaikan. Sholawat dan salam selalu terlimpahkan keharibaan Rosullah Muhammad SAW.

Emak dan Bapak Tercinta, sebagai tanda bukti, hormat dan rasa terima kasih yang tak terhingga kupersembahkan karya kecil ini kepada Emak dan Bapak yang telah memberi kasih sayang, segala dukungan dan cinta kasih yang tidak mungkin dapat kubalas dengan selembar kertas yang bertulisan kata cinta dan persembahan. Semoga ini menjadi langkah awal untuk membuat Emak dan Bapak bahagia karan kusadar selama ini belum bisa berbuat lebih. Untuk Emak dan Bapak yang selalu membuatku termotivasi dan selalu menyirami kasih sayang, selalu mendoakanku, selalu sabar menasehatiku menjadi lebih baik, Terima Kasih Emak.., Terima Kasih Bapak.

Untuk embak-embakku dan adikku, tiada yang paling mengharukan saat kumpul kalian, walaupun sering bertengkar tapi hal itu selalu menjadi warna yang tak akan bisa tergantikan, terimakasih atas doa dan bantuan selama ini, hanya karya kecil ini yang dapat aku persembahkan. Maaf belum bisa menjadi panutan yang baik seutuhnya, tapi aku akan menjadi yang terbaik untuk kalian semua..

Buat sahabat- sahabatku Ashabul Qohwah terimakasih banyak atas bantuan, doa, nasehat, hiburan, kekeluargaan, ojekkan, ejekkan dan semangat yang kalian berikan hingga saat ini, aku tak akan melupakan semua yang telah kalian berikan selama ini. Untuk sahabat seperjuangan seluruh sahabat kelas IT-G, terimakasih telah menjadi tempat dan sandaran saat pengerjaan tugas akhir ini sehingga dapat terselesaikan.

Untuk teman yang istimewa Winda Wahyu Affandini, terimakasih atas sayang, perhatian dan kesabaranmu yang telah memberikanku semangat, bantuan dan inspirasi dalam menyelesaikan tugas akhir ini. Semoga dan semoga disegerakan. Terimakasih banyak “ndook”..

Bapak Aminudin, dan Bapak Sofyan Arifianto selaku dosen pembimbing tugas akhir saya, terimakasih banyak pak..., saya sudah dibantu selama ini, sudah dinasehati, sudah diajari, saya tidak akan lupa atas bantuan dan kesabaran dari bapak. Terima kasih banyak untuk semua ilmu, didikan dan pengalaman yang sangat berarti yang telah kalian berikan kepada kami.

Seluruh pengajar di Teknik Informatika UMM yang telah mengajarkan ilmu kepada penulis dan tak akan pernah dapat dibalas oleh penulis. Bapak dan ibu dosen lah yang telah menempa diri penulis sehingga menjadi sekarang. Semoga Allah Subhanahu wa Ta'ala juga membalas seluruh jasa bapak dan ibu. Amin.

Untuk semua pihak yang tidak tersebut yang sudah membantu selama proses pengerjaan Tugas Akhir ini saya ucapkan terimakasih sebanyak banyaknya. Semoga Allah SWT membalas semua kebaikannya. Aamiin..



## KATA PENGANTAR



*Assalamu 'alaikum Warohmatullohi. Wabarokatuh.*

Syukur Alhamdulillah Segala puji bagi Allah SWT yang telah melimpahkan rahmat, taufik serta hidayahNya, sehingga penulis dapat menyelesaikan skripsi yang berjudul:

“ANALISA MODIFIKASI ALGORITMA RC4 MENGGUNAKAN TWO  
STATE TABLES DAN INITIAL STATE UNTUK PENGAMANAN FILE”

Skripsi ini merupakan salah satu syarat untuk memperoleh gelar Sarjana Komputer pada Jurusan Teknik Informatika, Fakultas Teknik Universitas Muhammadiyah Malang

Peneliti menyadari masih banyak kekurangan dan keterbatasan dalam penulisan tugas akhir ini. Untuk itu, penulis sangat mengharapkan saran yang membangun agar tulisan ini dapat berguna untuk perkembangan ilmu pengetahuan kedepan.

Malang, 13 Juli 2018

Penulis

Barkie Hasni Azzaky

## DAFTAR ISI

LEMBAR PERSETUJUAN.....	i
LEMBAR PENGESAHAN .....	ii
LEMBAR PERNYATAAN .....	iii
ABSTRAK.....	
ABSTRACT.....	
LEMBAR PERSEMBAHAN .....	iv
KATA PENGANTAR .....	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR .....	x
DAFTAR TABEL.....	x
BAB I PENDAHULUAN	
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah .....	3
1.3 Tujuan Penelitian .....	3
1.4 Batasan Masalah.....	3
1.5 Metodologi Penelitian .....	4
1.5.1 Studi Pustaka.....	4
1.5.2 Analisa dan Perancangan Sistem .....	4
1.5.3 Implementasi.....	4
1.5.4 Pengujian dan Analisa.....	4
1.5.5 Penyusunan Laporan Tugas Akhir .....	5
1.6 Sistematika Penulisan.....	5
BAB II LANDASAN TEORI	
2.1 Kriptografi.....	7
2.2 Algoritma RC4 Standar .....	8
2.2.1 Mekanisme Kerja RC4 Standar.....	11
2.2.2 Key Scheduling Algorithm (KSA).....	11
2.2.3 Pseudo-Random Generation Algorithm (PRGA) .....	12
2.2.4 Keamanan Algoritma RC4.....	12
2.2.4.1 Brute Force Attack.....	12



2.2.4.2	<i>Bit Flipping Attack</i> .....	13
2.3	Modifikasi Algoritma RC4.....	13
2.3.1	Mekanisme Kerja Modifikasi Algoritma RC4.....	16
2.3.2	<i>Key Scheduling Algorithm</i> (KSA).....	17
2.3.3	<i>Pseudo-Random Generation Algorithm</i> (PRGA) .....	17
2.4	File.....	17
<b>BAB III ANALISIS DAN PERANCANGAN SISTEM</b>		
3.1	Analisa Masalah .....	18
3.2	Rancangan Algoritma RC4 Standar .....	18
3.2.1	Fase KSA ( <i>Key Scheduling Algorithm</i> ) pada RC4 Standar .....	19
3.2.2	Fase PRGA ( <i>Pseudo-Random Generation Algorithm</i> ) pada RC4 Standart .....	20
3.3	Rancangan Modifikasi Algoritma RC4 .....	21
3.3.1	Fase KSA ( <i>Key Scheduling Algorithm</i> ) pada Modifikasi RC4.....	22
3.3.2	Fase PRGA ( <i>Pseudo-Random Generation Algorithm</i> ) pada Modifikasi RC4.....	23
3.4	Rancangan Uji Keamanan.....	25
3.4.1	<i>Brute Force Attack</i> .....	25
3.4.2	<i>Bit Flipping Attack</i> .....	25
3.5	Perbedaan penghitungan algoritma RC4 standar dan modifikasi RC4 ..	26
<b>BAB IV IMPLEMENTASI DAN PENGUJIAN</b>		
4.1	Implementasi .....	36
4.1.1	Implementasi Perangkat Keras.....	36
4.1.2	Implementasi Perangkat Lunak.....	36
4.1.3	Implementasi Algoritma RC Standar .....	36
4.1.3.1	Implementasi fase KSA algoritma RC4 standar.....	37
4.1.3.2	Implementasi fase PRGA algoritma RC4 standar .....	38
4.1.4	Implementasi Algoritma Modifikasi RC4.....	38
4.1.4.1	Implementasi Fase KSA Modifikasi Algoritma RC4.....	39
4.1.4.2	Implementasi Fase PRGA Modifikasi Algoritma RC4 .....	40
4.1.5	Implementasi <i>Brute Force Attack</i> .....	41
4.1.6	Implementasi <i>Bit Flipping Attack</i> .....	43

4.2	Pengujian .....	45
4.2.1	Pengujian Penjadwalan Kunci.....	46
4.2.2.1	Pengujian Waktu Pembangkitan Kunci Algoritma RC4 Standar dan Modifikasi Algoritma RC4 .....	46
4.2.2	Pengujian Waktu Enkripsi.....	47
4.2.2.1	Pengujian Waktu Enkripsi Algoritma RC4 Standar.....	47
4.2.2.2	Pengujian Waktu Enkripsi Modifikasi Algoritma RC4.....	49
4.2.2.3	Analisa Perbandingan Waktu Enkripsi.....	51
4.2.3	Pengujian Waktu Dekripsi .....	51
4.2.3.1	Pengujian Waktu Dekripsi Algoritma RC4 Standar.....	52
4.2.3.2	Pengujian Waktu Dekripsi Modifikasi Algoritma RC4 .....	53
4.2.3.3	Analisa Perbandingan Waktu Dekripsi.....	55
4.2.4	Pengujian terhadap Perubahan Besar File.....	55
4.2.5	Pengujian Metode <i>Brute Force Attack</i> .....	57
4.2.5.1	Pengujian <i>Brute Force Attack</i> .....	57
4.2.5.2	Analisis Perbandingan <i>Brute Force Attack</i> .....	58
4.2.6	Pengujian Metode <i>Bit Flipping Attack</i> .....	59
4.2.5.1	Pengujian <i>Bit Flipping Attack</i> .....	59
4.2.5.2	Analisis Perbandingan <i>Bit Flipping Attack</i> .....	60
BAB V PENUTUP		
5.1	Kesimpulan.....	61
5.2	Saran .....	62
DAFTAR PUSTAKA .....		63
LAMPIRAN.....		64

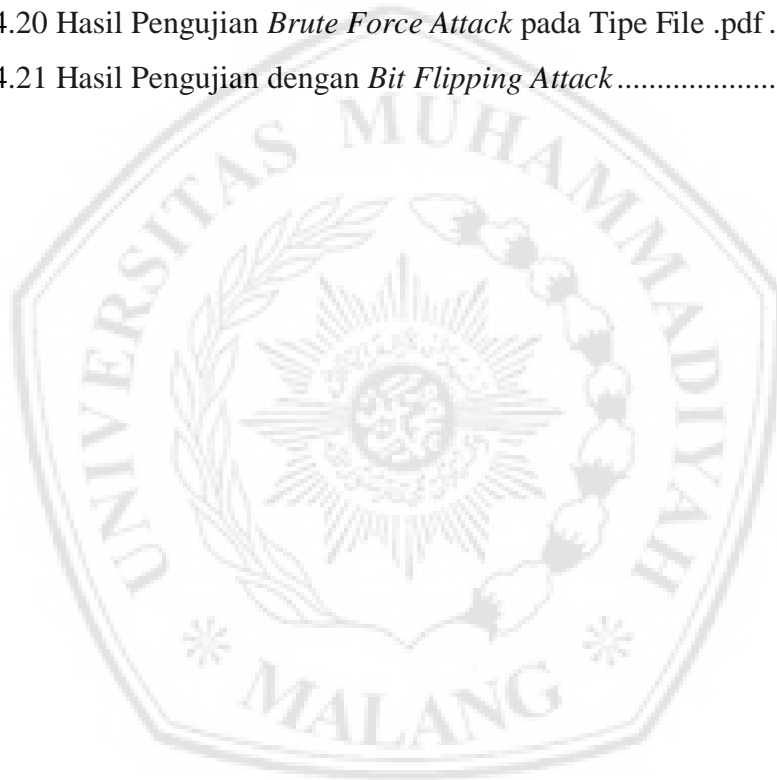
## DAFTAR GAMBAR

Gambar 2.1 Rangkaian Proses RC4 Stream Chiper.....	9
Gambar 3.1 Pseudocode Penjadwalan Kunci pada Algoritma RC4 Standar .....	19
Gambar 3.2 Flowchart Penjadwalan Kunci pada Algoritma RC4 Standar .....	20
Gambar 3.3 Pseudocode Proses Enkripsi pada RC4 Standar.....	21
Gambar 3.4 Flowchart Proses Enkripsi pada RC4 Standar.....	21
Gambar 3.5 Pseudocode Penjadwalan Kunci pada Modifikasi Algoritma RC4...	22
Gambar 3.6 Flowchart Penjadwalan Kunci pada Modifikasi Algoritma RC4.....	23
Gambar 3.7 Pseudocode Proses Enkripsi pada Modifikasi Algoritma RC4.....	24
Gambar 3.8 Flowchart Proses Enkripsi pada Modifikasi Algoritma RC4.....	24
Gambar 4.1 Potongan Sourcecode Fase KSA Algoritma RC4 Standar.....	37
Gambar 4.2 Potongan Sourcecode Fase PRGA Algoritma RC4 Standar .....	38
Gambar 4.3 Potongan Sourcecode Fase KSA Modifikasi Algoritma RC4 .....	39
Gambar 4.4 Potongan Sourcecode Fase PRGA Modifikasi Algoritma RC4.....	40
Gambar 4.5 Potongan Sourcecode Metode Uji <i>Brute Force Attack</i> .....	43
Gambar 4.6 Potongan Sourcecode Metode Uji <i>Bit Flipping Attack</i> .....	45

## DAFTAR TABEL

Tabel 3.1 Hasil Penghitungan Nilai K setiap Iterasi RC4 Standar .....	31
Tabel 3.2 Hasil Penghitungan Nilai K setiap Iterasi pada Modifikasi RC.....	33
Tabel 3.3 Nilai dari kode ASCII.....	33
Tabel 3.4 Hasil Chipertext pada Algoritma RC4 Standar.....	34
Tabel 3.5 Hasil Chipertext pada Modifikasi Algoritma RC4.....	34
Tabel 3.6 Perbandingan Mekanisme Kerja Algoritma RC4 Standar dan Modifikasi Algoritma RC4.....	34
Tabel 4.1 Hasil Pengujian Penjadwalan Kunci Algoritma RC4 Standar .....	46
Tabel 4.2 Hasil Pengujian Penjadwalan Kunci Modifikasi Algoritma RC4.....	46
Tabel 4.3 Hasil Pengujian Waktu Enkripsi Algoritma RC4 Standar pada Tipe File .txt.....	48
Tabel 4.4 Hasil Pengujian Waktu Enkripsi Algoritma RC4 Standar pada Tipe File .docx/doc .....	48
Tabel 4.5 Hasil Pengujian Waktu Enkripsi Algoritma RC4 Standar pada Tipe File .pdf .....	48
Tabel 4.6 Hasil Pengujian Waktu Enkripsi Modifikasi Algoritma RC4 pada Tipe File .txt .....	49
Tabel 4.7 Hasil Pengujian Waktu Enkripsi Modifikasi Algoritma RC4 pada Tipe File .docx/doc.....	50
Tabel 4.8 Hasil Pengujian Waktu Enkripsi Modifikasi Algoritma RC4 pada Tipe File .pdf .....	50
Tabel 4.9 Hasil Pengujian Waktu Dekripsi Algoritma RC4 Standar pada Tipe File .txt.....	52
Tabel 4.10 Hasil Pengujian Waktu Dekripsi Algoritma RC4 Standar pada Tipe File .docx/doc .....	52
Tabel 4.11 Hasil Pengujian Waktu Dekripsi Algoritma RC4 Standar pada Tipe File .pdf .....	53
Tabel 4.12 Hasil Pengujian Waktu Dekripsi Modifikasi Algoritma RC4 pada Tipe File .txt .....	53

Tabel 4.13 Hasil Pengujian Waktu Dekripsi Modifikasi Algoritma RC4 pada Tipe File .docx/doc.....	54
Tabel 4.14 Hasil Pengujian Waktu Dekripsi Modifikasi Algoritma RC4 pada Tipe File .pdf .....	54
Tabel 4.15 Perubahan Besar File Hasil Enkripsi File .txt .....	55
Tabel 4.16 Perubahan Besar File Hasil Enkripsi File .docx/doc.....	56
Tabel 4.17 Perubahan Besar File Hasil Enkripsi File .pdf.....	56
Tabel 4.18 Hasil Pengujian <i>Brute Force Attack</i> pada Tipe File .txt .....	57
Tabel 4.19 Hasil Pengujian <i>Brute Force Attack</i> pada Tipe File .docx/doc.....	57
Tabel 4.20 Hasil Pengujian <i>Brute Force Attack</i> pada Tipe File .pdf .....	58
Tabel 4.21 Hasil Pengujian dengan <i>Bit Flipping Attack</i> .....	59



## DAFTAR PUSTAKA

- [1] Zain, Ruri Hartika. “PERANCANGAN DAN IMPLEMENTASI CRYPTOGRAPHY DENGAN METODE ALGORITMA RC4 PADA TYPE FILE DOCUMENT DENGAN MENGGUNAKAN BAHASA PEMROGRAMAN VISUAL BASIC 6.0” *Jurnal Processor* Vol. 8 No. 1 2013.
- [2] Jindal, Poonam dan Brahmjit Singh. “Performance Analysis of Modified RC4 Encryption Algorithm” *International Conference on Recent Advances and Innovations in Engineering (ICRAIE)* 2014.
- [3] Xue, Pie, Tao Li, and Han Dong. “GB-RC4: Effective brute force attack on RC4 algorithm using GPU”. *International Green and Sustainable Computing Conference (IGSCC)* 2016.
- [4] Puspitasari, Amelia, Ari Moesriami Barmawi dan Tjokorda Agung Budi W. “Penanganan Bit Flipping Attack (BFA) pada Sistem Kriptografi RC4”. Program Studi Teknik Informatika Institut Teknologi Telkom.
- [5] Searan, Sura M. dan Sagheer, Ali M. “ Modification of RC4 Algorithm by using Two State Table and Initial State Factoral” *I. J. Computer Network and Information Security (IJCNIS)* 2016.
- [6] Sadikin, Rifki. 2012. “*Kriptografi Untuk Keamanan Jaringan dan Implementasinya Dalam Bahasa Java*”. Yogyakarta: CV ANDI OFFSET.
- [7] Ariyus, Dony. 2005. “*Kriptografi Keamanan Data dan Komunikasi*”. Penerbit: GRAHA ILMU.
- [8] Ariyus, Dony. 2008. “*Pengantar Ilmu Kriptografi : Teori Analisis dan Implementasi*”. Yogyakarta: CV ANDI OFFSET.
- [9] Arintamy, Vivien Septyaningtyas, Cahyani, Niken Dwi Wahyu dan Mulyana , Asep “ ANALISIS ALGORITMA RC4 SEBAGAI METODE ENKRIPSI WPA-PSK PADA SISTEM KEAMANAN JARINGAN WIRELESS LAN” *e.Proceeding of Engineering: Vol.1 No.1* 2014.
- [10] Hammod, M. M., K. Yoshigoe, and A. M. Sagheer. “RC4-2S: RC4 Stream Cheaper with Two State Tables”. *Information Technology Convergence, Lecture Notes in Electrical Engineering*. 2013
- [11] Fithria, Naila. “Jenis-Jenis Serangan terhadap kriptografi” *Teknik Informatika Institut Teknologi Bandung*. 2017.

## BIOGRAFI PENULIS

Nama : Barkie Hasni Azzaky  
NIM : 201310370311299  
TTL : Lamongan, 13 Desember 1993  
Alamat Asal : Sidomukti Brondong Lamongan  
Email : zacky.vengeance.zv@gmail.com  
No. HP : 081336334948

No	Nama Sekolah	Mulai	Sampai
1.	SD Negeri Sidomukti	1999	2006
2.	SMPM 12 Sendangagung	2006	2009
3.	MA Al-Ishlah Paciran	2009	2012
4.	Universitas Muhammadiyah Malang	2013	2018